

## Office Action Summary

Application No.

09/490,941

Applicant(s)

CZAJKOWSKI ET AL.

Examiner

Ronald F. Sulpizio

Art Unit

2132

The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM  
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 25 January 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claims \_\_\_\_\_ are subject to restriction and/or election requirement.

RECEIVED  
AUG 01 2005  
Technology Center 2100

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 January 2000 is/are objected to by the Examiner.
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved.
- 12) ☐ The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

### Attachment(s)

- 15) ☒ Notice of References Cited (PTO-892)
- 16) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 17) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_
- 18) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 19) ☐ Notice of Informal Patent Application (PTO-152)
- 20) ☐ Other:

## DETAILED ACTION

### ***Allowable Subject Matter***

1. Claim 7 is not allowed but could be if the 35 USC Sec. 112 rejections were overcome. The closest prior art to Claim 7 is Hice et al. (Hice, G.F. and Wold, S.H., *DMS Prologue to the Government E-Mail Revolution*, 1995, JG. Van Dyke & Associates, Inc.) which teaches:

A method for efficient encryption and decryption of Internet, Intranet, or e-mail messages, comprising the steps of;

- encrypting a message at a sending unit which is to be sent to a receiving unit using an integrated circuit embedded with algorithm located within said sending unit (Hice et al. p. 120);
- appending to the message at said sending unit the receiver's unencrypted IP address (Hice et al. p. 84 and 120 where the P1/P3/P7 envelope includes an unencrypted IP address of the recipient);
- appending to said message the receiver's encrypted IP address (Hice et al. p. 84 where the IP address is in the encrypted P772 header);
- said sending unit sends said encrypted message with said unencrypted IP address and said encrypted IP address (Hice et al. p.84 where the DMS message format contains all these features);
- receiving unit with an integrated circuit embedded with an encryption algorithm located within said receiving unit receives said encrypted message with said unencrypted IP address and said encrypted IP address using a receiving unit (Hice

Art Unit: 2132

et al. p. 121 and 122 where the FORTEZZA Card is used to receive encrypted DMS messages and decrypt them);

- receiving unit decrypts said encrypted IP address, storing said decrypted IP address in a register built into said integrated circuit embedded encryption algorithm located within receiving unit (Hice et al. p. 121 and 122 where the FORTEZZA Card is used to receive encrypted DMS messages with headers and decrypt them);

However, Hice et al. fails to teach:

- receiving unit stores said unencrypted IP address in a register built into said integrated circuit embedded with an encryption algorithm located within receiving unit;
- means for comparing said register storing unencrypted IP address to said register storing decrypted IP address;
- receiving unit decrypts said message if said register storing unencrypted IP address matches said register storing encrypted IP address;
- means for halting decryption process if said register storing unencrypted IP address does not match said register storing encrypted IP address.

### ***Drawings***

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "56" has been used to designate both "send message through private network" and "send message through network". Correction is required.

Art Unit: 2132

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 30, 32, 34, 36, and 38. Correction is required.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 10, 12, 14, 16, and 18. Correction is required.

***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 3-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Correction is required for the following:

- Claims 3 and 4 are process claims dependent from an apparatus claim.
- Claims 5 and 7 are method claims with apparatus elements.
- Claim 6 is unclear from which claim or combination of claims it depends.

***Claim Objections***

7. Claims 1, 3, and 5 are objected to because of the following informalities: the term "digital bit arrays" is not defined in the specification. Appropriate correction is required.

***Specification***

8. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 1, 3, and 5 refer to "digital bit arrays" which are not mentioned in the specification.

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hice et al. (Hice, G.F. and Wold, S.H., *DMS Prologue to the Government E-Mail Revolution*, 1995, JG. Van Dyke & Associates, Inc.).

**Claim 1**

Hice et al. teaches an apparatus for efficient encrypting and decrypting Internet, Intranet, or e-mail messages, comprising:

Art Unit: 2132

- an integrated electronic circuit, said circuit physically located within a computer communication device (Hice et al. p. 122; where the communication device is a PCMCIA card reader and the Fortezza PCMCIA card comprises an integrated electronic circuit).
- said circuit embedded with a random private cipher key generator (Hice et al. p. 120 and 122 where all crypto algorithms are embedded on the Capstone chip);
- said circuit embedded with asymmetric encryption algorithms (Hice et al. p. 122; where the Key Encryption Algorithm is an asymmetric encryption algorithm);
- said circuit embedded with symmetric encryption algorithms (Hice et al. p. 121; where Skipjack is a symmetric encryption algorithm);
- said circuit embedded with asymmetric decryption algorithms (Hice et al. p. 122; where the Key Encryption Algorithm is an asymmetric decryption algorithm);
- said circuit embedded with symmetric decryption algorithms (Hice et al. p. 121; where Skipjack is a symmetric decryption algorithm);.

Hice et al. fails to teach a digital bit array.

Official notice is taken that it is old and well known in the computer arts for an integrated circuit to be embedded with a common digital bit array/pre-loaded data to get the advantage of initializing a circuit. It would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Hice et al., then

Art Unit: 2132

not modify it, to get this advantage (See Hice et al. p. 122 describing the ability of the Fortezza Card to store data).

### Claim 2

Hice et al. teaches an apparatus wherein a circuit is located external of a computer communication device, and means for connecting said externally located circuit to said communication device (Hice et al. p. 122 where the FORTEZZA PCMCIA card is a mobile device readily insertable into a PCMCIA Card reader.).

### Claim 3

Hice et al. teaches a process to permit access to said encryption and decryption circuit recited in claim 1, wherein user access to said circuit further comprises:

- means for converting multiple user defined passwords into digital bit arrays (Hice et al. p. 33 describing PIN entry into a FORTEZZA PCMCIA card);
- means for programming said digital bit arrays into a non-volatile register located within said circuit (Hice et al. p. 122 describing the ability of the Fortezza Card to store data);
- means for verifying future user request to access said circuit with said stored digital bit arrays (Hice et al. p. 33 describing PIN entry into a FORTEZZA PCMCIA card);
- means for permitting user access to said circuit upon verification of user defined password with stored digital bit array (Hice et al. p. 33 describing PIN entry into a FORTEZZA PCMCIA card);

Art Unit: 2132

- means for denying access to said circuit upon lack of verification of user defined password with stored digital bit array (Hice et al. p. 33 describing PIN entry into a FORTEZZA PCMCIA card).

#### Claim 4

Hice et al. teaches a process to bypass said encryption and decryption circuit recited in claim 1, comprising means for said computer communication device operating without accessing said circuit, thereby said communications device operating unencrypted (Hice et al. p.33 describing a FORTEZZA PCMCIA card which can be removed from a PCMCIA card reader/communications device and PCMCIA card reader still being inherently functional).

#### Claim 5

Hice et al. teaches a method of sending encrypting Internet, Intranet, or e-mail messages, comprising the steps of:

- encrypting a message using an integrated circuit embedded with encryption algorithms (Hice et al. p. 121; where Skipjack is a symmetric encryption algorithm);
- said integrated circuit further embedded with random private cipher key generator (Hice et al. p. 122 where all crypto algorithms are embedded on the Capstone chip);
- appending an encrypted message header to said encrypted message, said message header encrypted using a receiver's public encryption key (Hice et al. p. 86 and p.120 where the encryption process includes a Message Encryption Key (MEK) that



Art Unit: 2132

is used to encrypt a message header and the receiver's public key is used to encrypt the MEK);

- said encrypted message header further comprising the sender's private signature cipher key and common digital bit array (Hice et al. p.120 where the sender's private cipher key is the MEK and the digital bit array is an array of data);
- means for transmitting said encrypted message header and said encrypted message to receiver over Internet (Hice et al. p. 121 where E-mail is the means),
- means for transmitting said encrypted message header and said encrypted message to receiver over Intranet (Hice et al. p. 121 where E-mail is the means),
- means for transmitting said encrypted message header and said encrypted message to receiver by e-mail (Hice et al. p. 121 where SMTP or X.400 E-mail is used);
- means for transmitting said encrypted message header and said encrypted message to receiver through wireless communication medium (Hice et al. p.49, Fig. 3-1, and p. 51 where the Defense Messaging System (DMS) uses hand-held, spread spectrum radio tranceivers).

Hice et al. fails to teach a digital bit array.

Official notice is taken that it is old and well known in the computer arts for an integrated circuit to be embedded with a common digital bit array to get the advantage of having a memory to store data (e.g. a user's private keys, public keys, authorizations, clearance level, and privileges, data storage key and executable programs). It would

Art Unit: 2132

have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Hice et al., then not modify it, to get this advantage (See Hice et al. p. 122 describing the ability of the Fortezza Card to store data).

#### Claim 6

Hice et al teaches a method of receiving and decrypting an encrypted message comprising the steps of;

- means for receiving an encrypted message header and encrypted message header and an encrypted message over Internet (Hice et al. p. 121 where E-mail is the means);
- means for receiving an encrypted message header and encrypted message header and an encrypted message over Intranet (Hice et al. p. 121 where E-mail is the means);
- means for receiving an encrypted message header and encrypted message header and an encrypted message by e-mail (Hice et al. p. 121 where SMTP or X.400 E-mail is used);
- means for receiving an encrypted message header and encrypted message header and an encrypted message through wireless communication medium (Hice et al. p.49, Fig. 3-1, and p. 51 where the Defense Messaging System (DMS) uses hand-held, spread spectrum radio tranceivers).;
- receiver gain access to decrypting integrated circuit as recited in claim 2 (Hice et al. p. 33 describing PIN entry into a FORTEZZA PCMCIA card);

Art Unit: 2132

- means for integrated circuit to decrypt and validate common digital bit array located in message header (Hice et al. p. 33 describing PIN entry into a FORTEZZA PCMCIA card);
- means for integrated circuit to decrypt sender's private signature cipher (Hice et al. p. 121 where the FORTEZZA Card is used to decrypt data);
- means for sender's private signature cipher key to permit access to decrypting integrated circuit for decryption of message (Hice et al. p. 121 where the FORTEZZA Card is used to decrypt data);

Hice et al. fails to teach:

- means for deleting sender's private signature cipher key from memory of receiver's computer;
- means for preventing receiver from viewing, saving, copying, or retaining sender's private signature cipher key.

Official notice is taken that it is old and well known in the cryptographic arts to discard a symmetric key once it is used and not reuse it but for the reaccessing of the item encrypted therefrom to get the advantage of more secure communications – repeat use of keys can lead to compromise of confidential data. It would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Hice et al., then not modify it, to get this advantage.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ronald F. Sulpizio whose telephone number is (703) 308-2391. The examiner can normally be reached on FF.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod R. Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-5065 for After Final communications.

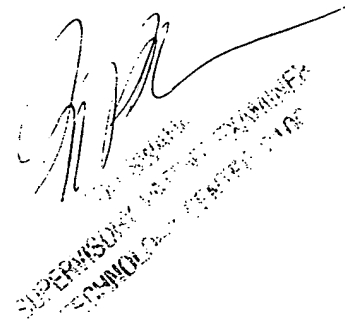
Art Unit: 2132

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.



Ronald F. Sulpizio  
Examiner  
Art Unit 2132

rfs  
March 14, 2001



SUPERVISORY PATENT EXAMINER  
COMMUNICATIONS SECTION

□

2835  
3 (10-96)  
651-0031  
MMERCE

Substitute for form 1449B/PTO

**Complete if Known**

*(use as many sheets as necessary)*

Sheet 1 of 1

Application Number	09/49041
Filing Date	01-25-2000
First Named Inventor	Czajkowski
Group Art Unit	
Examiner Name	
Attorney Docket Number	MA

RECEIVED

MAY 11 2000

OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS **Group 2700**

[illegible]

Examiner  
Signature

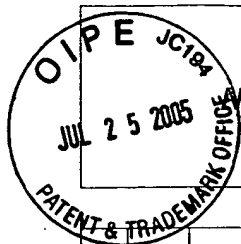
Date  
Considered

11 MAR 01

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

**Burden Hour Statement:** This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:** Assistant Commissioner for Patents, Washington, DC 20231.



# Notice of References Cited

Application/Control N

09/490.941

Applicant(s)/Patent Under  
Reexamination  
CZAJKOWSKI ET AL.

Examiner

Ronald F. Sulpizio

Art Unit

2132

Page 1 of 1

## U.S. PATENT DOCUMENTS

*		Document Number		Date MM-YYYY	Name	Classification	
		Country	Code-Number-Kind Code				
	A	US-	4924513-A	05-1990	Herbison et al.	713	161
	B	US-	5416842-A	05-1995	Aziz	380	30
	C	US-	5657390-A	08-1997	Elgamal et al.	713	151
	D	US-	-				
	E	US-	-				
	F	US-	-				
	G	US-	-				
	H	US-	-				
	I	US-	-				
	J	US-	-				
	K	US-	-				
	L	US-	-				
	M	US-	-				

RECEIVED  
AUG 01 2005  
Technology Center 2100

## FOREIGN PATENT DOCUMENTS

*		Document Number		Date MM-YYYY	Country	Name	Classification	
		Country	Code-Number-Kind Code					
	N	-	-					
	O	-	-					
	P	-	-					
	Q	-	-					
	R	-	-					
	S	-	-					
	T	-	-					

## NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)					
	U	Hice, G.F. and Wold, S.H., DMS Prologue to the Government E-Mail Revolution, 1995, JG. Van Dyke & Associates, Inc..					
	V						
	W						
	X						

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)

Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

# BEST AVAILABLE COPY

Form PTO 948 (Rev. 5-98)

U. S. DEPARTMENT OF COMMERCE - Patent and Trademark Office

Application No. \_\_\_\_\_

## NOTICE OF DRAFTSPERSON'S PATENT DRAWING REVIEW

The drawing(s) filed (insert date) \_\_\_\_\_ are:

A. ☐ approved by the Draftsperson under 37 CFR 1.84 or 1.152.

B. ☐ objected to by the Draftsperson under 37 CFR 1.84 or 1.152 for the reasons indicated below. The Examiner will require submission of new, corrected drawings when necessary. Corrected drawing must be submitted according to the instructions on the back of this notice.

1. DRAWINGS. 37 CFR 1.84(a): Acceptable categories of drawings:  
Black ink. Color.

\_\_\_\_ Color drawings are not acceptable until petition is granted.

Fig(s) \_\_\_\_\_

\_\_\_\_ Pencil and non black ink not permitted. Fig(s) \_\_\_\_\_

2. PHOTOGRAPHS. 37 CFR 1.84 (b)

\_\_\_\_ 1 full-tone set is required. Fig(s) \_\_\_\_\_

\_\_\_\_ Photographs not properly mounted (must use bristol board or photographic double-weight paper). Fig(s) \_\_\_\_\_

\_\_\_\_ Poor quality (half-tone). Fig(s) \_\_\_\_\_

3. TYPE OF PAPER. 37 CFR 1.84(e)

\_\_\_\_ Paper not flexible, strong, white, and durable.

Fig(s) \_\_\_\_\_

\_\_\_\_ Erasures, alterations, overwritings, interlineations, folds, copy machine marks not accepted. Fig(s) \_\_\_\_\_

\_\_\_\_ Mylar, velum paper is not acceptable (too thin).

Fig(s) \_\_\_\_\_

4. SIZE OF PAPER. 37 CFR 1.84(f): Acceptable sizes:

\_\_\_\_ 21.5 cm x 29.7 cm (DIN size A3)

\_\_\_\_ 21.5 cm x 33.0 cm (DIN size A4)

\_\_\_\_ 21.5 cm x 35.5 cm (DIN size A5)

\_\_\_\_ 21.5 cm x 38.0 cm (DIN size A6)

\_\_\_\_ 21.5 cm x 39.0 cm (DIN size A7)

\_\_\_\_ 21.5 cm x 40.0 cm (DIN size A8)

\_\_\_\_ 21.5 cm x 41.0 cm (DIN size A9)

\_\_\_\_ 21.5 cm x 42.0 cm (DIN size A10)

\_\_\_\_ 21.5 cm x 43.0 cm (DIN size A11)

\_\_\_\_ 21.5 cm x 44.0 cm (DIN size A12)

\_\_\_\_ 21.5 cm x 45.0 cm (DIN size A13)

\_\_\_\_ 21.5 cm x 46.0 cm (DIN size A14)

\_\_\_\_ 21.5 cm x 47.0 cm (DIN size A15)

\_\_\_\_ 21.5 cm x 48.0 cm (DIN size A16)

\_\_\_\_ 21.5 cm x 49.0 cm (DIN size A17)

\_\_\_\_ 21.5 cm x 50.0 cm (DIN size A18)

\_\_\_\_ 21.5 cm x 51.0 cm (DIN size A19)

\_\_\_\_ 21.5 cm x 52.0 cm (DIN size A20)

\_\_\_\_ 21.5 cm x 53.0 cm (DIN size A21)

\_\_\_\_ 21.5 cm x 54.0 cm (DIN size A22)

\_\_\_\_ 21.5 cm x 55.0 cm (DIN size A23)

\_\_\_\_ 21.5 cm x 56.0 cm (DIN size A24)

\_\_\_\_ 21.5 cm x 57.0 cm (DIN size A25)

\_\_\_\_ 21.5 cm x 58.0 cm (DIN size A26)

\_\_\_\_ 21.5 cm x 59.0 cm (DIN size A27)

\_\_\_\_ 21.5 cm x 60.0 cm (DIN size A28)

\_\_\_\_ 21.5 cm x 61.0 cm (DIN size A29)

\_\_\_\_ 21.5 cm x 62.0 cm (DIN size A30)

\_\_\_\_ 21.5 cm x 63.0 cm (DIN size A31)

\_\_\_\_ 21.5 cm x 64.0 cm (DIN size A32)

\_\_\_\_ 21.5 cm x 65.0 cm (DIN size A33)

\_\_\_\_ 21.5 cm x 66.0 cm (DIN size A34)

\_\_\_\_ 21.5 cm x 67.0 cm (DIN size A35)

\_\_\_\_ 21.5 cm x 68.0 cm (DIN size A36)

\_\_\_\_ 21.5 cm x 69.0 cm (DIN size A37)

\_\_\_\_ 21.5 cm x 70.0 cm (DIN size A38)

\_\_\_\_ 21.5 cm x 71.0 cm (DIN size A39)

\_\_\_\_ 21.5 cm x 72.0 cm (DIN size A40)

\_\_\_\_ 21.5 cm x 73.0 cm (DIN size A41)

\_\_\_\_ 21.5 cm x 74.0 cm (DIN size A42)

\_\_\_\_ 21.5 cm x 75.0 cm (DIN size A43)

6. VIEWS. 37 CFR 1.84(h)

\_\_\_\_ REMINDER: Specification may require revision to correspond to drawing changes.

\_\_\_\_ Partial views. 37 CFR 1.84(h)(2)

\_\_\_\_ Brackets needed to show figure as one entity.

Fig(s) \_\_\_\_\_

\_\_\_\_ Views not labeled separately or properly.

Fig(s) \_\_\_\_\_

\_\_\_\_ Enlarged view not labeled separately or properly.

Fig(s) \_\_\_\_\_

7. SECTIONAL VIEWS. 37 CFR 1.84 (h)(3)

\_\_\_\_ Hatching not indicated for sectional portions of an object.

Fig(s) \_\_\_\_\_

8. ARRANGEMENT OF VIEWS. 37 CFR 1.84(i)

\_\_\_\_ Words do not appear on a horizontal, left-to-right fashion when page is either upright or turned so that the top becomes the right side, except for graphs. Fig(s) \_\_\_\_\_

9. SCALE. 37 CFR 1.84(k)

\_\_\_\_ Scale not large enough to show mechanism without crowding when drawing is reduced in size to two-thirds in reproduction.

Fig(s) \_\_\_\_\_

10. CHARACTER OF LINES, NUMBERS, & LETTERS. 37 CFR 1.84(j)

\_\_\_\_ Lines, numbers & letters not uniformly thick and well defined, clean, durable, and black (poor line quality). Fig(s) \_\_\_\_\_

11. SHADING. 37 CFR 1.84(m)

\_\_\_\_ Solid black areas pale. Fig(s) \_\_\_\_\_

\_\_\_\_ Solid black shading not permitted. Fig(s) \_\_\_\_\_

\_\_\_\_ Shade lines, pale, rough and blurred. Fig(s) \_\_\_\_\_

12. NUMBERS, LETTERS, & REFERENCE CHARACTERS. 37 CFR 1.84(p)

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

\_\_\_\_ Numbers and letters not uniform in size, style, or color.

Fig(s) \_\_\_\_\_

13. LEAD LINES. 37 CFR 1.84(q)

\_\_\_\_ Lead lines cross each other. Fig(s) \_\_\_\_\_

\_\_\_\_ Lead lines missing. Fig(s) \_\_\_\_\_

14. NUMBERING OF SHEETS OF DRAWINGS. 37 CFR 1.84(t)

\_\_\_\_ Sheets not numbered consecutively, and in Arabic numerals beginning with number 1. Sheet(s) \_\_\_\_\_

15. NUMBERING OF VIEWS. 37 CFR 1.84(u)

\_\_\_\_ Views not numbered consecutively, and in Arabic numerals, beginning with number 1. Fig(s) \_\_\_\_\_

16. CORRECTIONS. 37 CFR 1.84(w)

\_\_\_\_ Corrections not made from prior PTO-948

dated \_\_\_\_\_

17. DESIGN DRAWINGS. 37 CFR 1.152

\_\_\_\_ Surface shading shown not appropriate. Fig(s) \_\_\_\_\_



# A Brief Summary of Some Significant Rule Changes

\*Unless otherwise specified in the rule, the effective date for the PBG-FINAL RULE is November 7, 2000.

## Amendment Practice (37 CFR 1.121)•

- Specification/Claims
  - Amendment by paragraph replacement or rewritten claim in clean form
  - Marked-up version showing changes must be supplied

See § 1.121 Slides on PBG-FINAL RULE Webpage for suggested amendment FORMAT (Optional now; mandatory March 1, 2001)

## Small Entity Status (37 CFR 1.27) - FORMS NO LONGER REQUIRED (Eff. Sept. 8, 2000):

- Mere written assertion (e.g., use check box on Application Transmittal Forms) is acceptable

## Abstract and Title Length (37 CFR 1.72)

- Abstract now limited to 150 words (PBG)
- Title now limited to 500 characters (AIPA)

## Application Data Sheet (ADS) (37 CFR 1.76) NEW

- • • • • Use of ADS encouraged for more accurate capture of bibliographic data. Data in ADS not needed in declaration.

## After Allowance Practice (37 CFR 1.85(c) and 1.136)

- No extensions of time permitted to file corrected or formal drawings

## Elimination of Issue Fee Preauthorizations (37 CFR 1.311)

- Preauthorizations prior to Notice of Allowance no longer permitted

## Rocket Docket Established for Designs (37 CFR 1.155)

- Extra submissions plus \$900 fee is required

## Proof of Authority of Legal Representative (37 CFR 1.44) THIS RULE HAS BEEN DELETED. (Eff. Sept. 8, 2000):

- Oath/Dec. (§1.63) should identify legal rep for deceased/incapacitated inventor

## Parts of Applications on CD-R or CD-ROM (37 CFR 1.52 (e), 1.58, 1.96 & 1.821)

- Large tables, computer program listings, and bio-sequences now allowed on CD

# Patent Business Goals Final Rule

65 Fed. Reg. 54604 (September 8, 2000)

1238 Off. Gaz. Pat. Office 77 (September 19, 2000)



USPTO's PBG-FINAL RULE webpage has helpful related information at one location:  
<http://www.uspto.gov/web/offices/dcom/olia/pbg/index.html>

This site includes:  
a Listing of Affected Rules,  
Training & Implementation  
Materials including Training  
Slides, Q & A's, Summaries,  
Effective Date Chart, Forms  
Changed by Recent Rules, etc.

Contact:  
Bob Spar (703) 308-5107 or  
Hiram Bernstein (703) 305-8713  
for any PBG Change.

Joe Narcavage (703) 305-1795  
for 37 CFR 1.121  
Amendment Practice Changes

Eugenia Jones (703) 306-5586  
for 37 CFR 1.27 Small Entity  
Changes



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Patent and Trademark Office**  
ASSISTANT SECRETARY AND COMMISSIONER  
OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

Dear Patent and Trademark Office Customer:

The Technical Support Staff of Technology Center 2100 has undertaken continuous quality improvement efforts to ensure that the accompanying correspondence meets high quality standards, and focuses on good customer service. It is important to us that you are satisfied with the services we provide.

If the contents of the attached correspondence has any clerical omissions, e.g., missing references or pages, illegible text, other problems or concerns of this nature which you wish to bring to my attention, please call or fax me as soon as possible. I will take the appropriate action to expedite the necessary corrections.

A handwritten signature in cursive script, appearing to read "Verlene D. Green".

Verlene D. Green  
Head, Supervisory Legal Instruments Examiner  
Technology Center 2100  
(703) 305-4376

Fax No. (703) 308-9051 or (703) 308-9052

## **Attention: Policy on Returning Phone Calls**

A PTO-wide customer service standard is if a PTO employee being called is not available, they will return your call by the next business day, or, if you request, an alternate point of contact will be provided. Technology Center 2100 is committed to meeting this service standard. If you have called any employee in our Technology Center and have not received a return phone call within one (1) business day or have not been provided another point of contact, please contact the Technology Center at 703-306-5631. We ensure that you will receive a return phone call, from an employee with the ability to assist you, within four (4) business hours of this contact. We appreciate your help in assisting us to help you.

In The United States Patent and Trademark Office

Mailed 2000 April 19

Assistant Commissioner for Patents  
Washington, DC 20231

Certificate of Mailing

I certify that this correspondence will be deposited with the United States Postal Service as first class mail with proper postage affixed in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231, on the date below.

Items Included:

- 1 Information Disclosure Statement (2 sheets)
- 1 US Patent - Lewis (#5,761,306)
- 1 US Patent - Nakamura (#6,014,444)
- 1 US Patent - Coutts (#5,835,603)
- 1 PC Guardian datasheet
- 1 Return Postcard

4/19/00  
Date

David R. Czajkowski  
David Czajkowski

**FILING RECEIPT**

\*OC00000004996998\*


**UNITED STATES DEPARTMENT OF COMMERCE**  
**Patent and Trademark Office**

 Address: ASSISTANT SECRETARY AND  
 COMMISSIONER OF PATENT AND TRADEMARKS  
 Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/490,941	01/25/2000	2766	345	-	4	7	3

 David Czajkowski  
 Bernard Gudaitis  
 332 Alviso Way  
 Encinitas, CA 92024

Date Mailed: 03/17/2000

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

**Applicant(s)**
 David Czajkowski, Encinitas, CA ;  
 Bernard Gudaitis, Palos Verdes Estates, CA ;
**Continuing Data as Claimed by Applicant****Foreign Applications**

If Required, Foreign Filing License Granted 03/17/2000

**\*\* SMALL ENTITY \*\*****Title**

Encrypted internet and intranet communication device

**Preliminary Class**

713

Data entry by : ROBINSON, YOLANDA

Team : OIPE

Date: 03/17/2000



**LICENSE FOR FOREIGN FILING UNDER  
Title 35, United States Code, Section 184  
Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 36 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

**PLEASE NOTE the following information about the Filing Receipt:**

- The articles such as "a," "an" and "the" are not included as the first words in the title of an application. They are considered to be unnecessary to the understanding of the title.
- The words "new," "improved," "improvements in" or "relating to" are not included as first words in the title of an application because a patent application, by nature, is a new idea or improvement.
- The title may be truncated if it consists of more than 600 characters (letters and spaces combined).
- The docket number allows a maximum of 25 characters.
- If your application was submitted under 37 CFR 1.10, your filing date should be the "date in" found on the Express Mail label. If there is a discrepancy, you should submit a request for a corrected Filing Receipt along with a copy of the Express Mail label showing the "date in."

Any corrections that may need to be done to your Filing Receipt should be directed to:

Assistant Commissioner for Patents  
Office of Initial Patent Examination  
Customer Service Center  
Washington, DC 20231

David Czajkowski  
332 Alviso Way  
Encinitas, CA 92024

The following received today:

Patent Application for David Czajkowski and  
Bernard Gutaitis for "ENCRYPTED INTERNET AND  
INTRANET COMMUNICATION DEVICE",  
Consisting of 12 sheets of specifications, claims,  
and abstract, declaration signed 2000 January 25,  
4 sheets informal drawings, small entity declaration,  
and check #1745 for \$345.00.



In the United States Patent and Trademark Office

First Applicant: David Czajkowski

Second Applicant: Bernard Gudaitis

Title: " ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE"

Small Entity Declaration – Independent Inventor(s)

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 C.F.R. 1.9(c) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35 United States Code, to the Patent and Trademark Office with regard to my above-identified invention described in the specification filed herewith. I have not assigned, granted, conveyed, or licensed – and am under no obligation to under any contract or law to assign, grant, convey or license – any rights in the invention to either (a) ant person who could not be classified as an independent inventor under 37 C.F.R. 1.9(c) if that person had made the invention, or (b) any concern which would not qualify as either (i) a small business concern under 37 C.F.R. 1.9(d) or (ii) a nonprofit corporation under 37 C.F.R. 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed – or am under an obligation to under any contract or law to assign, grant, convey or license – any rights in the invention is listed below:

X  There is no such person, concern, or organization.

Any applicable person, concern, or organization is listed below:

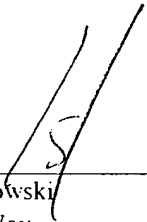
---

---

I acknowledge a duty to file, in the above application for patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fees or any maintenance fees due after the date on which the status of small entity is no longer appropriate. (37 CFR 1.28(b))

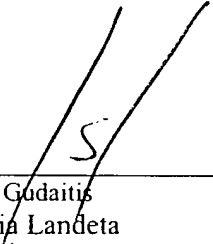
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the

knowledge that the willful false statements and the like so made punishable by fine or imprisonment, or both, under Title 18, United States Code, Section 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon, or any patent to which this verified statement is directed.



---

David Czajkowski  
332 Alviso Way  
Encinitas, CA 92024  
Dated 2000 January 25



---

Bernard Gudaitis  
1241 Via Landeta  
Palos Verdes, CA 90274  
Dated 2000 January 25



## Declaration for Utility Patent Application

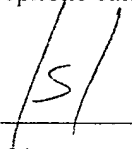
As below named inventor, I hereby declare that my residence, post office address, and citizenship are stated below next to my name and that I believe I am the original, first, and sole inventor (if only one name is listed below) or and original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention, the specification of which is attached hereto which has the following title:

**"ENCRYPTED INTERNET MODEM COMMUNICATIONS SYSTEM"**

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration. I acknowledge a duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that the willful false statements and the like so made punishable by fine or imprisonment, or both, under Title 18, United States Code, Section 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Please send correspondence and make telephone calls to the First Inventor below.

Signature: First Inventor  Date: 2000 January 25

Name: David Czajkowski

Mailing Address: 332 Alviso Way Phone: (760) 633-4450

Encinitas, CA 92024

Legal Residence: Encinitas, CA Citizenship: USA

Signature: Second Inventor  Date: 2000 January 25

Name: Bernard Gudaitis

Mailing Address: 1241 Via Landeta Phone: (310) 373-1633

Palos Verdes Estates, CA 90274

Legal Residence: Palos Verdes Estates Citizenship: USA

In The United States Patent and Trademark Office

Mailed 2000 January 25

Box Patent Application  
Assistant Commissioner for Patents  
Washington, DC 20231

Sir:

Please file the following enclosed patent application papers:

Applicant #1, Name: David Czajkowski

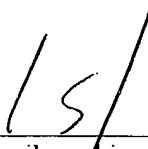
Applicant #2, Name: Bernard Gudaitis

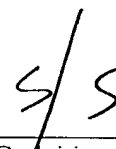
Title: "ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE"

- Specification, Claims, and Abstract: Nr. Of Sheets: 11
- Declaration: Date Signed: 2000 January 25
- Drawing(s): Nr. Of Sheets: Informal: 4
- Small Entity Declaration of Inventor(s)
- Check #1745 for the amount of \$ 345.00 for filing fee ( not more than three independent claims and twenty total claims are presented.
- Return Receipt Postcard Addressed to Applicant #1.

**Request Under MPEP section 707.07(j):** The undersigned, a pro se applicant, respectfully requests that if the Examiner finds patentable subject matter disclosed in this application, but feels that the Applicant's present claims are not entirely suitable, the Examiner draft one or more allowable claims for the applicant.

Very Respectfully,

  
\_\_\_\_\_  
David Czajkowski  
332 Alviso Way (Send Correspondence Here)  
Encinitas, CA 92024

  
\_\_\_\_\_  
Bernard Gudaitis  
1241 Via Landeta  
Palos Verdes Estates, CA 90274

**Express Mail Label #** \_\_\_\_\_

**Date Deposited 2000 January 25**

In The United States Patent and Trademark Office

Mailed 2000 January 25

Box Patent Application  
Assistant Commissioner for Patents  
Washington, DC 20231

**FEE TRANSMITTAL**

First Named Applicant: David Czajkowski

Title of Invention: "ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE"

Total Payment Enclosed (from Calculation Below): \$ 345.00      Check #1745

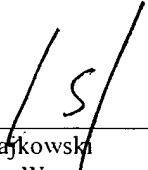
Sir:

Enclosed is the following small entity fee for the above patent application:

<b>Fee Code</b>	<b>Fee Description</b>	<b>Fee(\$)</b>
210	Basic Utility Appn. Filing Fee	\$345.00
203	Total Claims 7; Number of claims over 20: <u>0</u>	= 0
202	Total Indep. Claims 3; Number of Indep Claims over 3: <u>0</u>	= 0
	Subtotal (2)	= 0

**Total Payment Enclosed [Sum of Subtotal(1) and Subtotal(2)]**      \$345.00

Very Respectfully,

  
\_\_\_\_\_  
David Czajkowski  
332 Alviso Way  
Encinitas, CA 92024

David Czajkowski and Bernard Gudaitis

For

**TITLE: ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE**

**CROSS-REFERENCE TO RELATED APPLICATIONS**

Not Applicable

**BACKGROUND -- FIELD OF INVENTION**

This present invention relates a method for providing a secure encrypted computer communication channel across the Internet, more particularly, the use of e-mail access software and the addition of an integrated circuit embedded with several encryption algorithms to a communications device, thereby providing encryption/decryption capabilities.

**BACKGROUND – DESCRIPTION OF PRIOR ART**

Typical communication between two or more parties through the Internet 18 using a computer, 10 and 11 is accomplished through the use of a communications devices, 14 and 16 and communication software as referenced in FIG 1. A computer with communication capabilities, as reference in FIG 2 will utilize a communication controller 20 to interface with the Internet 22. The Internet consists of many public domain computers, electronic routers and switches, and computer servers generally accessible by the public. Accessing this network is not controlled by any individual organization and is not limited in any ways other than by protocol definitions (TCP, IP, etc).

Communication on the Internet between two parties can take place using two different methods:

1. *Sending data*: when one party groups a message and/or data package into a specific formatted sequence, attaches the Internet address, termed an Internet Protocol (IP) Address and then sends the message and IP Address to the Internet. The data is typically packetized using commercially available software and sent from the computer through the communication device onto the Internet.
2. *Accessing data*: when one party connects to a public or private database across the Internet by connecting to the database's website. Access is typically made by using the communication device to connect to the website's URL Address.

Originally, the security of these communications was not an issue as very few individuals possessed the necessary computer hardware or technical expertise to intercept the messages. However, the arrival of inexpensive personal computers and the explosion in the popularity of the Internet, in particular electronic commerce (e-commerce), prompted the development of computer communication security devices.

The existing method of security that presently exists is computer software programs that encrypt communication data between two users using encryption algorithms, such as the Blowfish algorithm. U.S. Pat. No. 6,014,444 relies on a cypher key approach for encryption. These methods involve using a key, known by both the sender and receiver, which is used by the encryption algorithm to encode the data into an unrecognizable format. The data is then passed from the sender to the receiver. After successful transmission, the receiver has an encrypted data package. The receiver must then get the key from the sender and use it to re-run the same decryption algorithm to decrypt the message. An example of this software is found in the 1999 PC Guardian Incorporated "Encryption Plus for Email" product datasheet.

The security of these software encryption systems may be compromised as the software (therefore the encryption algorithm) may be subject to computer hacking. Furthermore, the myriad of encryption software has led to incompatibilities. One encryption program is generally incompatible with a competing company's software. Therefore, the sender and the receiver must be using the same program. Lastly, once the encryption algorithm has been compromised, messages encrypted with the algorithm may easily be decrypted. A person located external to the communications network may intercept and decrypt the message if the software has been effectively "hacked".

A different security approach has involved the use of computer smart cards. U.S. Pat. No. 5,761,306 provides other improved methods of encryption involving a system of computers to exchange public keys over an insecure network. These systems rely on a combination of nodes that are implemented by a computer, smart card, a stored data card in combination with a publicly accessible node machine. This system, however, will still depend on the effectiveness of the underlying encryption software and require the user to possess a smart card to effectively operate. Additionally, these software encryption systems generally only provide single layer encryption, in that the entire message will be encrypted using one algorithm.

U.S. Pat. No. 5,835,603 describes a home banking system using an encrypted modem as part of its system. This system is similar to all standard encryption techniques, but differs from the present invention in that it does not specify asymmetric and symmetric encryption functions embedded into an integrated circuit. Additionally, it does not utilize an Internet IP Address as part of its encryption system and does not offer any solutions for decryption.

Therefore, it is further desirable to have the encryption algorithm encoded onto a integrated circuit within the communication device. As such, hacking into the encryption chip would require purchasing an encryption chip and reverse engineering the chip to the underlying physical operations. In addition, for a large number of electronic network users, the private keys should be securely transmitted over the network.

## **SUMMARY**

The present invention discloses an apparatus and method for providing secured information exchange through the Internet and Intranet, consisting of a computer communications device containing an integrated electronic circuit embedded with asymmetric and symmetric encryption/decryption algorithms.

According to the present invention, furthermore, there is provided a multiple step process which is added to existing standard Internet communication sequences for both sending and accessing data to implement the encryption procedure.

Other features of the present invention will become apparent from the accompanying drawings and from the detailed description which follows.

## **OBJECT AND ADVANTAGES**

The present invention provides advantages over existing prior art in that:

- (a) The inclusion of a hard wired integrated circuit containing embedded encryption algorithms into the computer communication device provides increased security over current software encryption systems. One wishing to discover the encryption algorithm would be required reverse engineer the chip down to the operational level (examine the gates and transistors comprising the chip function), as opposed to external program hacking to which a software-only system is susceptible. Such an effort would not generally be cost effective.
- (b) Secure automatic electronic private key transmission between sender and receiver.
- (c) The communication device with the integrated circuit, when installed in a computer, contains all the encryption hardware and software. No additional encryption technology is required to be purchased and installed.
- (d) The process accompanying the present invention when incorporated to existing Internet communication sequences will require verification of the receiver's Internet or IP address before transmitting the encrypted data. Current systems do not require verification of the recipient's Internet or IP address.

## **BRIEF DESCRIPTION OF THE DRAWING**

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals indicate similar elements and in which:

FIG 1 is a block diagram of a typical communication network.

FIG 2 is a block diagram of a computer with a communications device.

FIG 3 is a block diagram of an encryption/decryption communication device in accordance with an embodiment of the present invention.

FIG 4 is a flow chart of the encryption/decryption method in accordance with an embodiment of the present invention.

## **DETAILED DESCRIPTION OF THE PRESENT INVENTION**

The present invention contains all the functions necessary for secure communications in one physical device as referenced in figure 3. This device contains an encryption and decryption integrated circuit 30 that uses a combination of asymmetric and symmetric functions to encrypt and decrypt data. The encryption/decryption integrated circuit can be accessed by the user through a password protected user interface controller 32. This communication device also contains a signal processor 34 used to process the incoming and outgoing data. This may include multiplexing, de-multiplexing, modulating, demodulating, encoding, decoding, and error detection and correction. Memory 36 is included within the device for algorithm, control, and data storage. A network interface 38, electrical power 40, and a clock for internal timing 42 is also part of the communication device.

The present invention involves a multiple step process which is added to existing standard Internet communication sequences for both sending and accessing data. A primary private key is encrypted using a public/private key pair, then the remainder of the data is encrypted with a faster algorithm using another randomly generated primary key. An Encrypted Internet Communication System is required at both the sender and receiver for successful secure transmission. The verification process is completed using a set of software and hardware verification steps that unlock the encryption algorithm hardware to the receiver. The process involves a communication setup, a sender sequence and a receiver sequence. The process is as follows:

## Communication Setup

When the communication device and associated software is installed into the computer, the following sequence is followed to setup levels of security:

1. The software requests a password from the user, either the sender or receiver.
2. The software converts the password to a digital, electronic bit format and transfers the digitized password to the communication device hardware, which stores the password permanently into a non-volatile hardware register.

### Send Sequence

1. To access the encryption algorithm, the user must successfully re-enter the password into the software and matched in the hardware during the send sequence 44.
2. Sender requests encryption access from software.
3. Software asks for password from sender. (Steps 3 and 4 are optional).
4. Software compares password with previously stored password during the Communication Setup sequence of communication system. If matched, encryption algorithm is made available to sender. If not matched, encryption algorithm is not made available to sender. (Steps 3 and 4 are optional).
5. Data is passed through encryption hardware in communication device. The data encryption is performed in the following manner as referenced in figure 4:
  - a. the communication device accesses the receiver's public key. A Certification Authority (CA) is used to verify the receiver's public key 46.
  - b. the sender randomly generates its private key 48
  - c. the sender's private key is encrypted using the receiver's public key 50
  - d. the sender's data is encrypted using the sender's private key 52
  - e. the receiver's Internet Protocol's (IP) address is acted upon in one of the following ways:
    - i) the receiver's IP address is not encrypted
    - ii) a copy of the receiver's IP address is encrypted using a private key (different private key from the one encrypting the message) 54
  - f. the IP address, encrypted copy of the IP address (if ii is performed), encrypted private key, and encrypted message is transmitted as a message block to the receiver. If the IP address is encrypted the message block could be sent to the receiver through a private network to verify the receiver. If the IP address is not encrypted, the message block is sent to the receiver through normal channels 56.

### Receive Sequence



1. After message data received by receiver, receiver requests software to de-encrypt data 58.
2. Software requests a password to communication device; receiver enters password.
3. Software transfers receiver password to communication device. Compare of password is completed by communication device. If matched, de-encrypt sequence is allowed to continue. If not matched, sequence is halted and error message is passed back to software.
4. Software then sends a un-encrypted e-mail on to the Internet through the communication device that provides a return message to the same (receiver) IP Address. The message will include a unique code to signify a verification check (unique verification code) and the IP Address. Numerous techniques can be used to verify the e-mail has reached the actual Internet, such as, use of "Certification Authority", reading the Domain Name Server and returning verification data and/or use of a private server that provides a return of the e-mail with verification of reaching the Internet. In all cases, the message will return to the receiver IP Address along with the unique verification code.
5. If the receiver's IP address is verified then the encryption of the data can proceed.
6. Software then transfers data to communication device.
7. The receiver's private key (as part of its private/public key pair) is then used to decrypted the sender's private key 60.
8. Then the receiver uses the sender's private key to decrypt the message 62.
9. The receiver's communication device deletes the sender's private key 64.
10. The receiver's communication device sends a message receipt to the sender 66.

## **CONCLUSIONS, RAMIFICATIONS, AND SCOPE OF INVENTION**

Accordingly, the reader will see that the present invention provides multiple layer of encryption, yet will not impinge on the operational utility of the computer communications device. Furthermore, the apparatus and process outlined above prevents or efficiently deters external computer theft of sensitive information. Lastly, the apparatus and process may be upgraded with the addition of different algorithms.

While the above description contains many specifications, these specifications should not be construed as limitations on the scope or utility of the invention, but are presented to exemplify a preferred embodiment thereof.

Accordingly, the scope of the invention should be determined not by the embodiments presented, but by the appended claims and their legal equivalents.

## **CLAIMS**

1. An apparatus for efficient encrypting and decrypting Internet, Intranet, or e-mail messages, comprising:

an integrated electronic circuit, said circuit physically located within a computer communication device;

said circuit embedded with a common digital bit array;

said circuit embedded with a random private cypher key generator;

said circuit embedded with asymmetric encryption algorithms;

said circuit embedded with symmetric encryption algorithms;

said circuit embedded with asymmetric decryption algorithms;

said circuit embedded with symmetric decryption algorithms.

2. An apparatus as recited in claim 1, wherein said circuit is located external of said computer communication device, and means for connecting said externally located circuit to said communication device.

3. A process to permit access to said encryption and decryption circuit recited in claim 1, wherein user access to said circuit further comprises:

means for converting multiple user defined passwords into digital bit arrays;

means for programming said digital bit arrays into a non-volatile register located within said circuit;

means for verifying future user request to access said circuit with said stored digital bit arrays;

means for permitting user access to said circuit upon verification of user defined password with stored digital bit arrays;

means for denying access to said circuit upon lack of verification of user defined password with stored digital bit array.

4. A process to bypass said encryption and decryption circuit recited in claim 1, comprising means for said computer communication device operating without accessing said circuit, thereby said communications device operating unencrypted.

5. A method of sending encrypting Internet, Intranet, or e-mail messages, comprising the steps of :

encrypting a message using an integrated circuit embedded with encryption algorithms,

said integrated circuit further embedded with random private cypher key generator;

said integrated circuit further embedded with a common digital bit array;

appending an encrypted message header to said encrypted message, said message header encrypted using a receiver's public encryption key;

said encrypted message header further comprising the sender's private signature cypher key and a common digital bit array;

means for transmitting said encrypted message header and said encrypted message to receiver over Internet;

means for transmitting said encrypted message header and said encrypted message to receiver over Intranet;

means for transmitting said encrypted message header and said encrypted message to receiver by e-mail;

means for transmitting said encrypted message header and said encrypted message to receiver through wireless communication medium.

6. A method of receiving and decrypting an encrypted message as recited in claim 5, comprising the steps of :

means for receiving an encrypted message header and encrypted message header and an encrypted message over Internet;

means for receiving an encrypted message header and encrypted message header and an encrypted message over Intranet;

means for receiving an encrypted message header and encrypted message header and an encrypted message by e-mail;

means for receiving an encrypted message header and encrypted message header and an encrypted message through wireless communication medium;

receiver gain access to decrypting integrated circuit as recited in claim 2;

means for integrated circuit to decrypt and validate common digital bit array located in message header;

means for integrated circuit to decrypt sender's private signature cypher;

means for sender's private signature cypher key to permit access to decrypting integrated circuit for decryption of message;

means for deleting sender's private signature cypher key from memory of receiver's computer;

means for preventing receiver from viewing, saving, copying, or retaining sender's private signature cypher key.

7. A method for efficient encryption and decryption of Internet, Intranet, or e-mail messages, comprising the steps of:

encrypting a message at a sending unit which is to be sent to a receiving unit using an integrated circuit embedded with algorithm located within said sending unit;

appending to the message at said sending unit the receiver's unencrypted IP address;

appending to said message the receiver's encrypted IP address;

said sending unit sends said encrypted message with said unencrypted IP address and said encrypted IP address;

receiving unit with an integrated circuit embedded with an encryption algorithm located within said receiving unit receives said encrypted message with said unencrypted IP address and said encrypted IP address using a receiving unit;

receiving unit decrypts said encrypted IP address, storing said decrypted IP address in a register built into said integrated circuit embedded encryption algorithm located within receiving unit;

receiving unit stores said unencrypted IP address in a register built into said integrated circuit embedded with an encryption algorithm located within receiving unit;

means for comparing said register storing unencrypted IP address to said register storing decrypted IP address;

receiving unit decrypts said message if said register storing unencrypted IP address matches said register storing encrypted IP address;

means for halting decryption process if said register storing unencrypted IP address does not match said register storing encrypted IP address.

## **ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE**

**ABSTRACT:** A method and apparatus for providing multiple layer encrypted Internet, Intranet, or e-mail communication device communications. In particular, the process of encrypting Internet, Intranet, or e-mail messages with encryption algorithms embedded in integrated circuits incorporated into the communication device, with access to the encrypting circuit requiring a validation of a randomly generated cypher key and an user defined password.



**GUARDDOG COMMUNICATION, INC**  
1833 DIAMOND ST. SUITE 201  
SAN MARCOS, CA 92069  
(760) 744-8310

**BANK OF AMERICA, NA**  
LOS ANGELES, CA 90067-3101  
18-66/1220

1156

07/16/2001

PAY TO THE  
ORDER OF Assistant Commissioner of Patents

\$\*\*135.00

One Hundred Thirty-Five and 00/100\*\*\*\*\*

DOLLARS

MEMO Add'l independent claims; patent 09/490,941

⑈001156⑈ ⑆122000661⑆ 11510⑈08164⑈

*Dandygale*





**UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

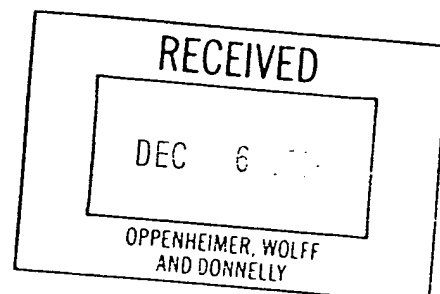
EXAMINER
----------

ART UNIT	PAPER NUMBER
----------	--------------

**DATE MAILED:**

**Please find below and/or attached an Office communication concerning this application or proceeding.**

**Commissioner of Patents and Trademarks**





UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS  
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

EXAMINER
----------

ART UNIT	PAPER NUMBER
----------	--------------

6

DATE MAILED:


**Notice of Non-Compliant Amendment (37 CFR 1.121)**

The amendment filed on 7-30-01 is considered non-compliant because it has not been submitted in the format required under 37 CFR 1.121, as amended on September 8, 2000 (see 65 Fed. Reg. 54603, Sept. 8, 2000 and 1238 O.G. 77, Sept. 19, 2000).

- ☒ The amendment does not include a clean version of the replacement paragraph/section. 37 CFR 1.121(b)(1)(ii)
- ☒ The amendment does not include a marked-up version of the replacement paragraph/section 37 CFR 1.121(b)(1)(iii)
- ☐ The amendment does not include a clean version of the amended claim(s). 37 CFR 1.121(c)(1)(i)
- ☐ The amendment does not include a marked-up version of the amended claim(s). 37 CFR 1.121(c)(1)(ii)

**For your convenience, attached to this correspondence is a copy of an informational flyer (MPEP Bookmark Bulletin on "Simplified Amendment Practice").**

Applicant is given a TIME PERIOD of ONE (1) MONTH or THIRTY (30) DAYS from the mailing date of this notice, whichever is longer, within which to submit an amendment in compliance with 37 CFR 1.121, effective March 1, 2001, in order to avoid abandonment. EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 C.F.R. 1.136(a).

  
Randy Harrison  
Legal Instruments Examiner

# Changes to the Patent Rules

October 20, 2000

Volume 1, Issue 3

This is the third in a series of Patent News Bulletins to assist you in keeping up to date with significant rule changes which affect your area. Keep this copy to use as a bookmark for your present MPEP, or view this bulletin again on the USPTO Website.



## Simplified Amendment Practice. Replacement paragraphs/sections/claims to be used. 37 CFR 1.121

The rule package "Changes to the Patent Business Goals - Final Rule," published in the Federal Register on September 8, 2000, 65 Fed. Reg. 54603 (Sept. 8, 2000), and the Official Gazette on September 19, 2000, 1238 Off. Gaz. Pat. Office 77 (September 19, 2000). The PBG rule package makes a number of revisions to Title 37.

The entire final rule may be found at the USPTO Website at <http://www.uspto.gov/web/offices/dcom/olia/pbg/index.html>.

Areas and individuals primarily affected by this rule change include:  
(1) Patent Examiners and Tech Support Staff in the Technology Centers  
(2) Office of Patent Publication

Any questions related to this change in practice should be directed to Joe Narcavage, Special Projects Exr., (703-305-1795) or Liz Dougherty, Legal Advisor, (703-306-3156) OPLA.



Mandatory compliance with the revised rule is not required until March 1, 2001. It is suggested that applicants adopt the revised procedures on or after November 7, 2000, in order to adjust to the changes in amendment practice.

Under the new amendment practice, amendments to the specification must be made by the submission of clean new or replacement paragraph(s), section(s), specification, or claim(s). This practice will provide a specification (including claims) in clean, or substantially clean, form that can be effectively captured and converted by optical character recognition (OCR) scanning during the patent printing process.

The new practice requires applicant to provide, in addition to the clean version of a replacement paragraph/section/claim, a marked-up version using applicant's choice of a conventional marking system to indicate the changes, which will aid the examiner in identifying the changes that have been made. The marked-up version must be based on the previous version and indicate (by markings) how the previous version has been modified to produce the clean version submitted in the current amendment. The term "previous version" means the version of record in the application as originally filed or from a previously entered amendment.

The following format is suggested in an amendment paper: (1) a clean version of each replacement paragraph/section/claim with clear instructions for entry; (2) starting on a separate page, any remarks/arguments (37 CFR 1.111); and (3) starting on a separate page, a marked-up

version entitled "Version with markings to show changes made."

Applicants will also be able to submit a clean set of all pending claims, consolidating all previous versions of pending claims from a series of separate amendments into a single clean version in a single amendment paper. This submission of a clean version of all of the pending claims will be construed as directing the cancellation of all previous versions of any pending claims. No marked-up version will be required to accompany the clean version where no changes other than the consolidation are being made.

The amended rule encourages issuance of applications with an examiner's amendment without practitioners/applicants having to file a formal amendment. Additions or deletions of subject matter in the specification, including the claims, may continue to be

made in an examiner's amendment at the time of allowance by instructions to make any change at a precise location in the specification or the claims. An examiner's amendment may incorporate a printed copy of a fax or e-mail amendment submitted by applicant. Only that part of the e-mail or fax directed to a clean version, or a portion of, a paragraph/claim to be added should be printed and attached to the examiner's amendment, with a paper copy of the entire e-mail or fax being entered in the file. The electronic version of the e-mail is not required to be saved once the printed e-mail (and any attachments) becomes part of the application file record.

*Amendment by  
paragraph/claim  
replacement in clean form.*

MPEP 714+ & 1302.04

Attachment for PTO-948 (Rev. 03/01, or earlier)  
6/18/01

The below text replaces the pre-printed text under the heading, "Information on How to Effect Drawing Changes," on the back of the PTO-948 (Rev. 03/01, or earlier) form.

INFORMATION ON HOW TO EFFECT DRAWING CHANGES

**1. Correction of Informalities -- 37 CFR 1.85**

New corrected drawings must be filed with the changes incorporated therein. Identifying indicia, if provided, should include the title of the invention, inventor's name, and application number, or docket number (if any) if an application number has not been assigned to the application. If this information is provided, it must be placed on the front of each sheet and centered within the top margin. If corrected drawings are required in a Notice of Allowability (PTOL-37), the new drawings **MUST** be filed within the **THREE MONTH** shortened statutory period set for reply in the Notice of Allowability. Extensions of time may **NOT** be obtained under the provisions of 37 CFR 1.136(a) or (b) for filing the corrected drawings after the mailing of a Notice of Allowability. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftsperson.

**2. Corrections other than Informalities Noted by Draftsperson on form PTO-948.**

All changes to the drawings, other than informalities noted by the Draftsperson, **MUST** be made in the same manner as above except that, normally, a highlighted (preferably red ink) sketch of the changes to be incorporated into the new drawings **MUST** be approved by the examiner before the application will be allowed. No changes will be permitted to be made, other than correction of informalities, unless the examiner has approved the proposed changes.

**Timing of Corrections**

Applicant is required to submit the drawing corrections within the time period set in the attached Office communication. See 37 CFR 1.85(a)

Failure to take corrective action within the set period will result in **ABANDONMENT** of the application.

## ASSIGNMENT

WHEREAS, I, David Czajkowski, residing at 332 Alviso Way, Encinitas, CA 92024 USA, a citizen of the United States of America, co-invented certain new and useful improvements disclosed in an application for United States Letters Patent titled **Encrypted Internet Modem Communications System**, and executed me on even date herewith; and

WHEREAS, GuardDog Communication, Inc., a Nevada Corporation, located at 332 Alviso Way, Encinitas, CA 92024 USA (hereinafter, together with any successors, legal representatives or assigns thereof, called "Assignee"), wants to acquire the entire right, title and interest in and to said improvements and application:

NOW, THEREFORE, in consideration of the sum of One Dollar (\$1.00) to me in hand paid, and other good and valuable consideration, the receipt of which is hereby acknowledged, have sold, assigned, transferred and set over, and do hereby sell, assign, transfer and set over to Assignee the entire right, title and interest in and to said improvements, and said application and all divisions, substitutes and continuations thereof, and all United States Letters Patents which may be granted thereon and all reissues and extensions thereof, and all priority rights under the International Convention for the Protection of Industrial Property for every member country, and all applications for patents (including related rights such as utility-model registrations, inventor's certificates, and the like) heretofore or hereafter filed for said improvements in any foreign countries, and all patents (including all extensions, renewals and reissues thereof) granted for said improvements in any foreign countries; and each hereby authorizes and requests the United States Commissioner of Patents and Trademarks, and any officials of foreign countries whose duty is to issue patents on applications as aforesaid, to issue all patents for said improvements to Assignee in accordance with the terms of this assignment:

AND I HEREBY covenant that I have full right to convey the entire interest herein assigned, and that I have not executed, and will not execute, any agreement in conflict herewith;

AND I HEREBY further covenant and agree that I will communicate to Assignee any facts known to me respecting said improvements, and testify in any legal proceedings, sign all lawful papers, execute all divisional continuation, substitute and reissue applications, make all rightful oaths and generally do everything possible to aid Assignee to obtain and enforce proper patent protection for said improvements in all countries.

THIS ENTIRE ASSIGNMENT inures to the benefit of Assignee, its successors and assigns, and is binding upon me, my heirs, successors and legal representatives.

IN TESTIMONY WHEREOF, I hereunto set my hand this 2 day of August, 2000.

David Czajkowski

STATE OF CALIFORNIA )  
 ) ss.  
COUNTY OF SAN DIEGO )

On this 21<sup>st</sup> day of AUGUST, 2008 before me DONALD C. SCARFF, the undersigned Notary Public, personally appeared David Czajkowski, personally known to me (or proved to me on the basis of satisfactory evidence) to be the person whose name is subscribed to the within instrument and acknowledged to me that he executed the same.

Notary Public

Donald C. Pitt

[illegible]

## ASSIGNMENT

WHEREAS, I, David Czajkowski, residing at 332 Alviso Way, Encinitas, CA 92024 USA, a citizen of the United States of America, co-invented certain new and useful improvements disclosed in an application for United States Letters Patent titled **Encrypted Internet Modem Communications System**, and executed me on even date herewith; and

WHEREAS, GuardDog Communication, Inc., a Nevada Corporation, located at 332 Alviso Way, Encinitas, CA 92024 USA (hereinafter, together with any successors, legal representatives or assigns thereof, called "Assignee"), wants to acquire the entire right, title and interest in and to said improvements and application:

NOW, THEREFORE, in consideration of the sum of One Dollar (\$1.00) to me in hand paid, and other good and valuable consideration, the receipt of which is hereby acknowledged, have sold, assigned, transferred and set over, and do hereby sell, assign, transfer and set over to Assignee the entire right, title and interest in and to said improvements, and said application and all divisions, substitutes and continuations thereof, and all United States Letters Patents which may be granted thereon and all reissues and extensions thereof, and all priority rights under the International Convention for the Protection of Industrial Property for every member country, and all applications for patents (including related rights such as utility-model registrations, inventor's certificates, and the like) heretofore or hereafter filed for said improvements in any foreign countries, and all patents (including all extensions, renewals and reissues thereof) granted for said improvements in any foreign countries; and each hereby authorizes and requests the United States Commissioner of Patents and Trademarks, and any officials of foreign countries whose duty is to issue patents on applications as aforesaid, to issue all patents for said improvements to Assignee in accordance with the terms of this assignment:

AND I HEREBY covenant that I have full right to convey the entire interest herein assigned, and that I have not executed, and will not execute, any agreement in conflict herewith;

AND I HEREBY further covenant and agree that I will communicate to Assignee any facts known to me respecting said improvements, and testify in any legal proceedings, sign all lawful papers, execute all divisional continuation, substitute and reissue applications, make all rightful oaths and generally do everything possible to aid Assignee to obtain and enforce proper patent protection for said improvements in all countries.

THIS ENTIRE ASSIGNMENT inures to the benefit of Assignee, its successors and assigns, and is binding upon me, my heirs, successors and legal representatives.

IN TESTIMONY WHEREOF, I hereunto set my hand this 2 day of August, 2000.

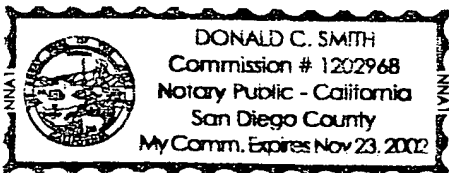
David Czajkowski

STATE OF CALIFORNIA )  
 ) ss.  
COUNTY OF SAN DIEGO . )

On this 21<sup>st</sup> day of AUGUST, 2008 before me DONALD C. SCARFF, the undersigned Notary Public, personally appeared David Czajkowski, personally known to me (or proved to me on the basis of satisfactory evidence) to be the person whose name is subscribed to the within instrument and acknowledged to me that he executed the same.

Notary Public

Ronald C. Felt



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**